# ABSTRACT OF THE DISCLOSURE

A malware detection system seeking to identify computer viruses, worms, Trojans, banned files and the like acts to determine from the file name, file size and storage location of a computer file being tested, whether that computer file potentially matches a specific known malware free computer file stored within a list of such specific known malware free computer files. If a match occurs indicating that the candidate computer file is potentially the specific known malware free computer file, then this is confirmed by calculating a checksum of the candidate computer file and comparing this against a stored corresponding checksum of the specific known malware free computer file. If these checksums match, then the candidate computer file can be passed as clean without requiring further time consuming malware detection scanning.

[Figure 4]